United States Cyber Command

What It Takes To Operate In Cyberspace

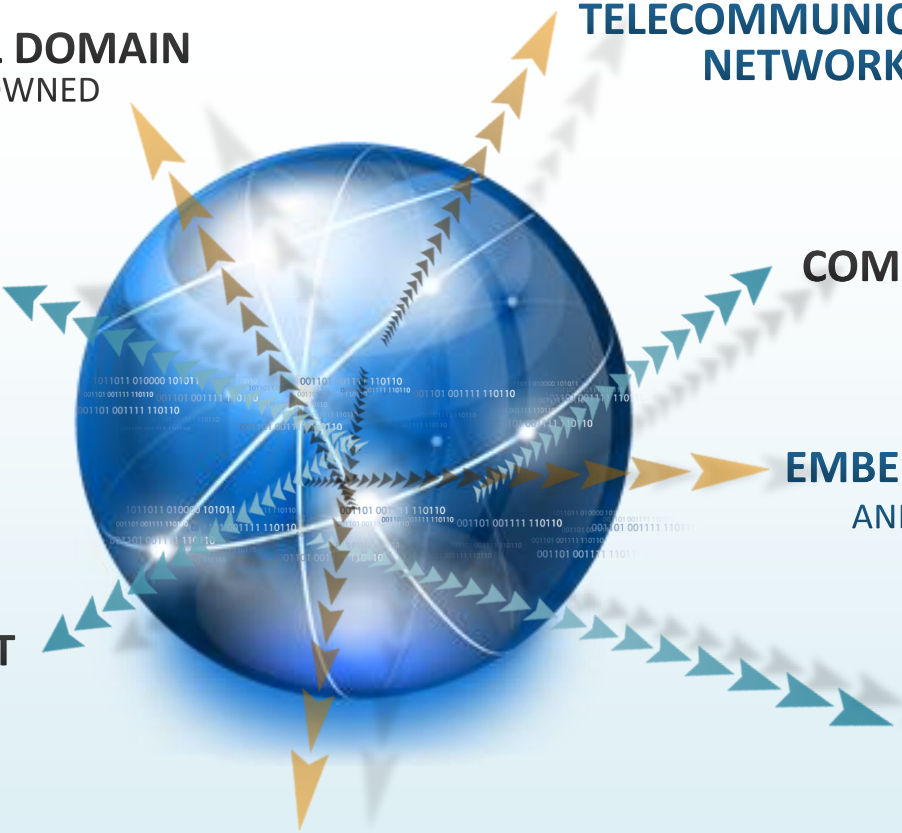
May 2014

Major General Tom Thomas, USAF DE ANG

National Guard Assistant to the Commander, USCYBERCOM and the National Security Agency

The overall classification of this brief is: **UNCLASSIFIED**

Nature of Cyberspace



MANMADE GLOBAL DOMAIN
THAT IS PRIVATELY OWNED

TELECOMMUNICATIONS
NETWORKS

PROGRAMMING CODE
AND PROTOCOLS DEFINE
RULES OF THE DOMAIN

COMPUTER SYSTEMS

EMBEDDED PROCESSORS
AND CONTROLLERS

VIRTUAL ENVIRONMENT

INTERNET

TOOLS, TACTICS AND PROCEDURES
EVOLVING AT NETSPEED

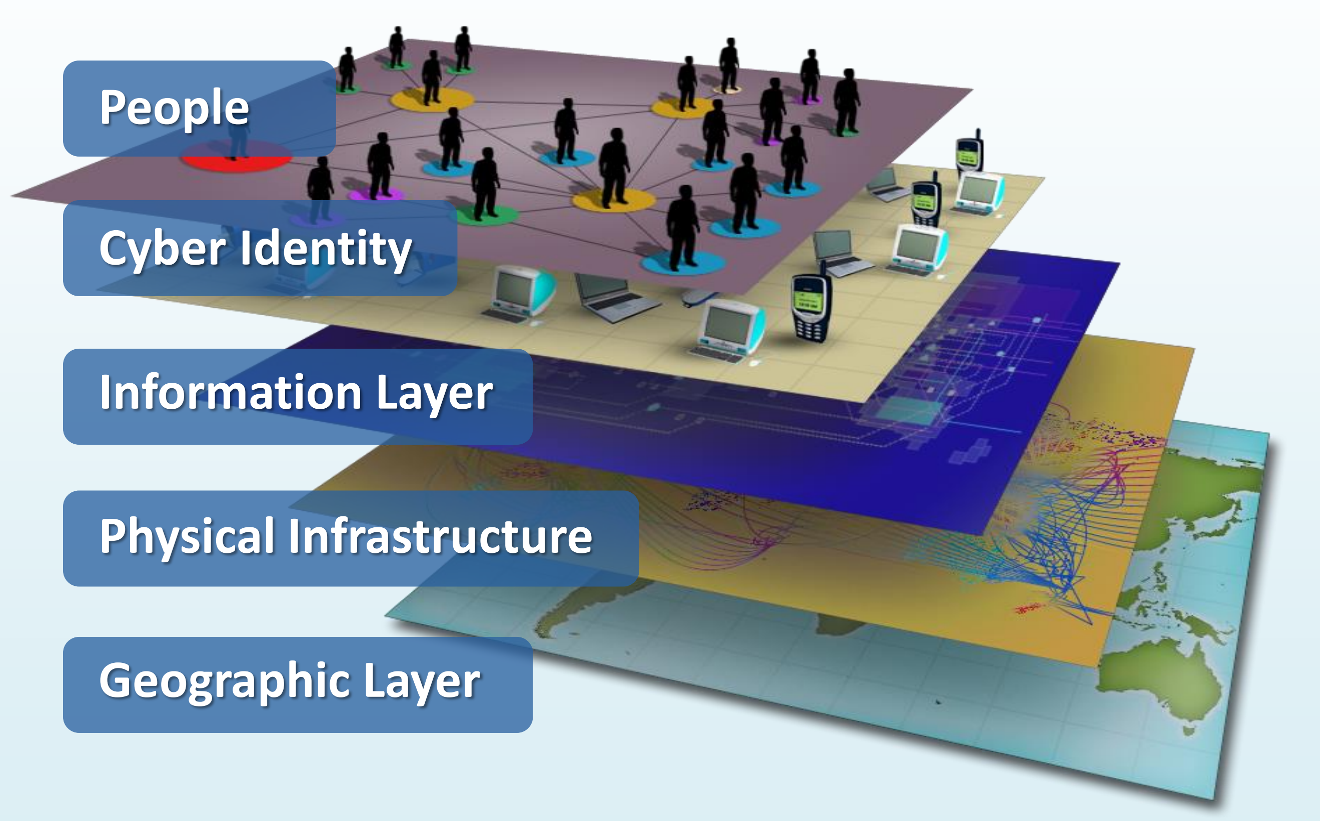
Success in this domain means being smarter, more creative, faster, and stealthier than our opponent.

The Cyber Environment

Cyberspace is where the Nation stores its treasure (intellectual property) and its wealth (money)

Benefits:

- National security
- Economic competiveness
- Public safety
- Civil liberties & privacy



People

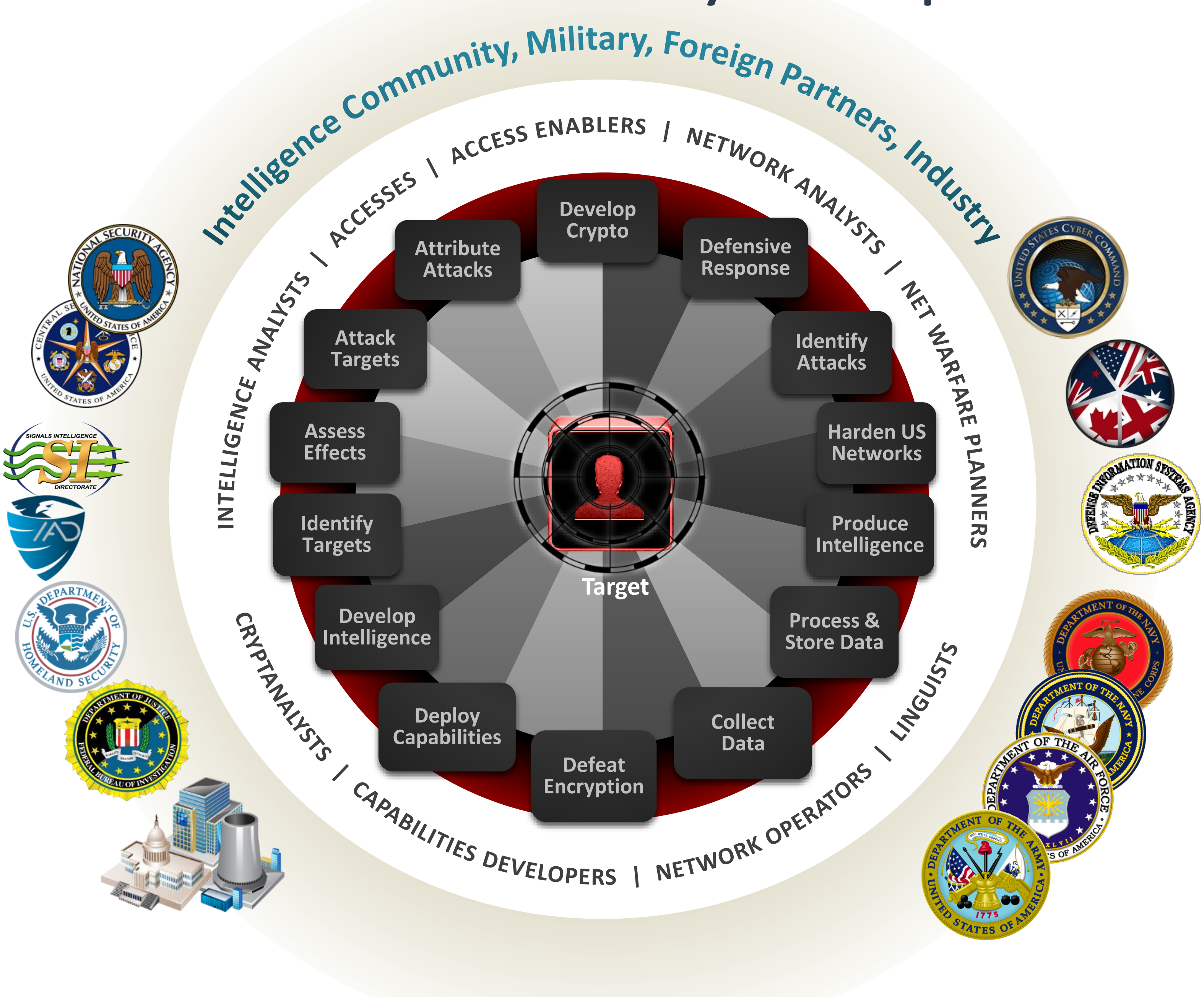
Cyber Identity

Information Layer

Physical Infrastructure

Geographic Layer

What it Takes to do Cyber Operations



Intelligence Community, Military, Foreign Partners, Industry

ACCESS ENABLERS | NETWORK ANALYSTS | NET WARFARE PLANNERS | LINGUISTS | NETWORK OPERATORS | CAPABILITIES DEVELOPERS | CRYPTANALYSTS | INTELLIGENCE ANALYSTS | ACCESSES |

Develop Crypto

Defensive Response

Identify Attacks

Harden US Networks

Produce Intelligence

Process & Store Data

Collect Data

Defeat Encryption

Deploy Capabilities

Develop Intelligence

Identify Targets

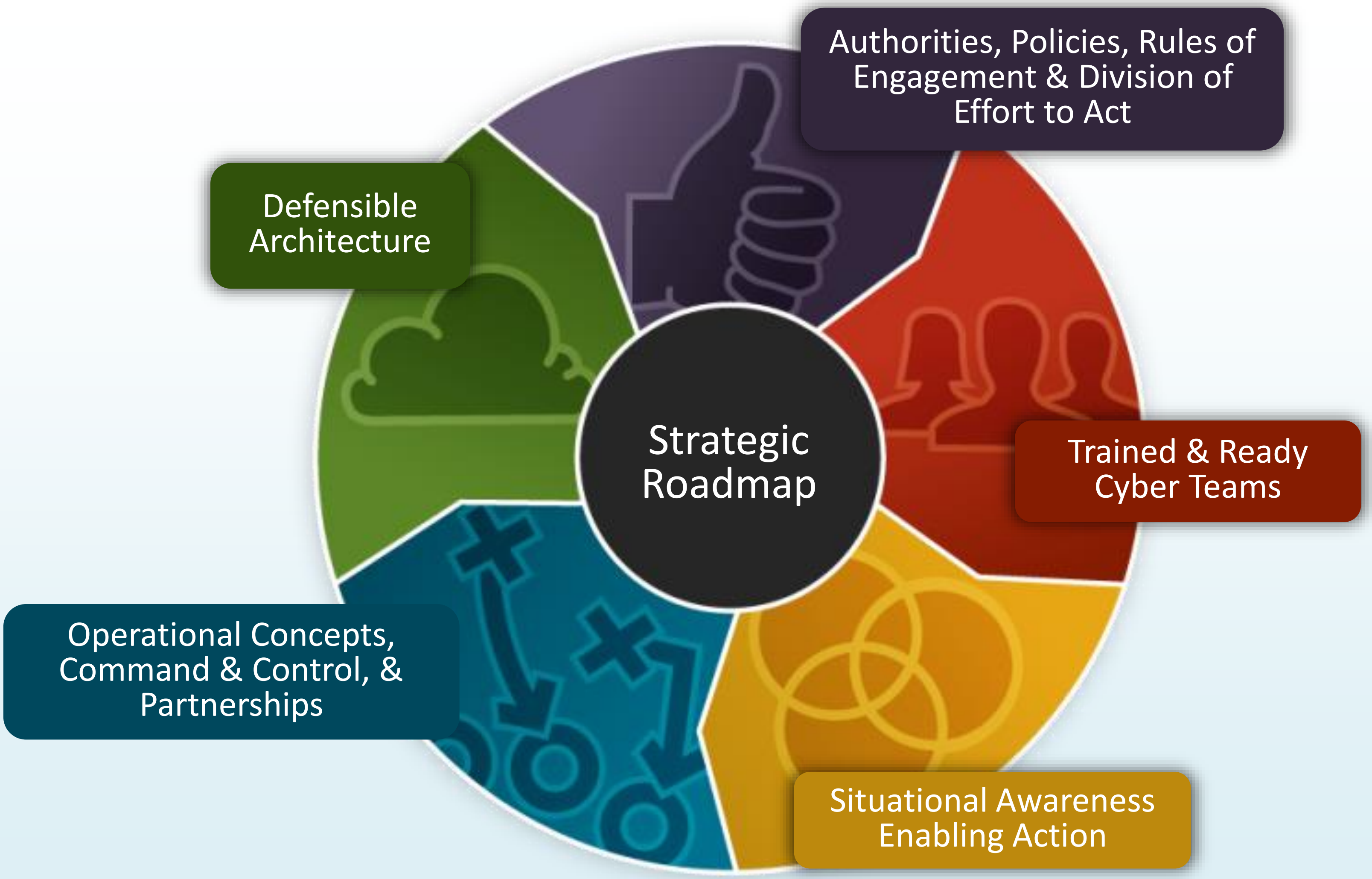
Assess Effects

Attack Targets

Attribute Attacks

Target

US Cyber Command
Five Strategic Priorities for Operating in Cyberspace



Strategic Roadmap

Authorities, Policies, Rules of Engagement & Division of Effort to Act

Trained & Ready Cyber Teams

Situational Awareness Enabling Action

Operational Concepts, Command & Control, & Partnerships

Defensible Architecture

Change Continues at Exponential Rates

Library of Congress = 10 Terabytes

At best transmission line speed:

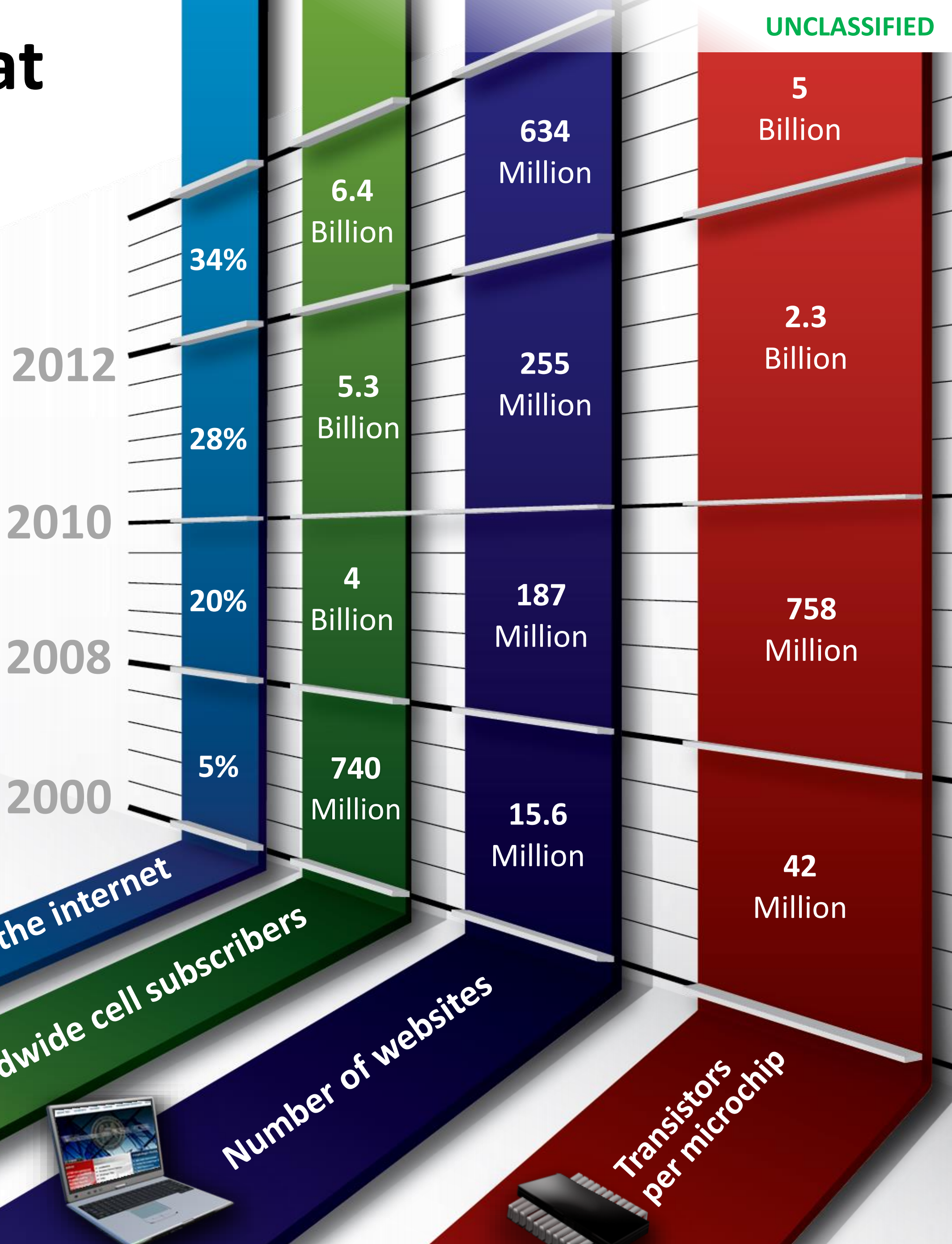
- 1998 = 16.5 days
- 2013 = .00008 seconds

10 Billion Mobile Devices Projected by 2016

(1.4 per person on the planet)

Facebook

- Launch, 2004
- Reaches1 Billion Users, 2012



Convergence Opportunities & Vulnerabilities

Convergence means we all operate on the same network…

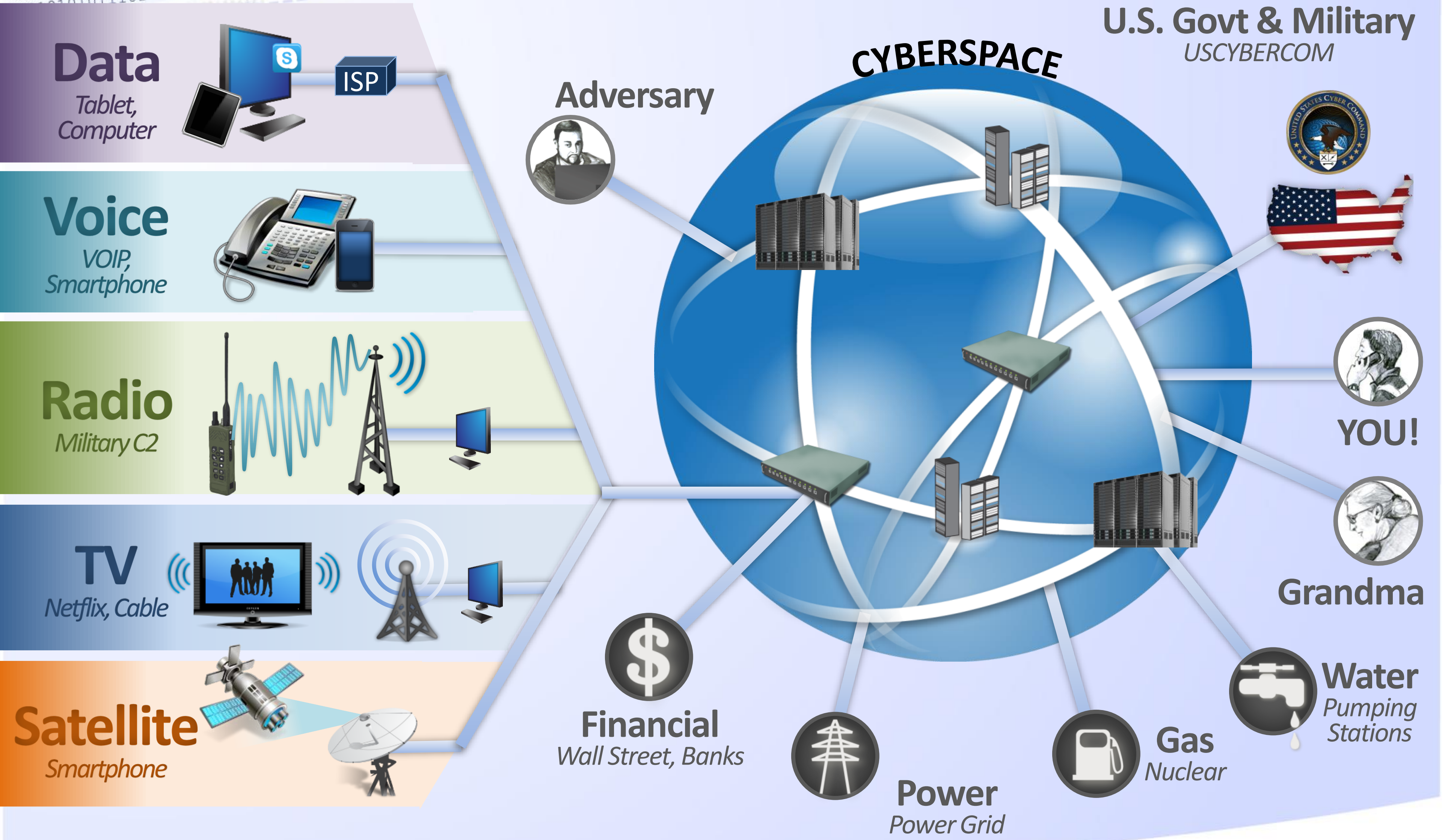
Opportunities

- Gathering Information; planning cyber operations
- Possible attribution of a cyber attack
- Intelligence collection & production more efficient & effective
- Ability to maneuver in cyberspace

Vulnerabilities

- An effective cyber attack against the right sector could be devastating to the US economy
- Our adversaries are exploiting us; we must defend our networks

Convergence Opportunities & Vulnerabilities



Data
Tablet, Computer

ISP

Voice
VOIP, Smartphone

Radio
Military C2

TV
Netflix, Cable

Satellite
Smartphone

Adversary

CYBERSPACE

U.S. Govt & Military
USCYBERCOM

YOU!

Grandma

Water
Pumping Stations

Gas
Nuclear

Power
Power Grid

Financial
Wall Street, Banks

THREAT ACTORS

THREAT ACTORS

FOREIGN INTELLIGENCE

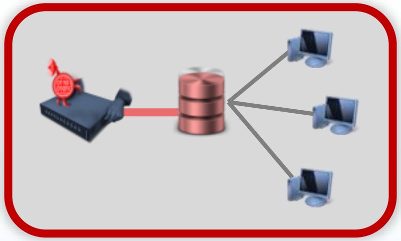
HACKTIVISTS

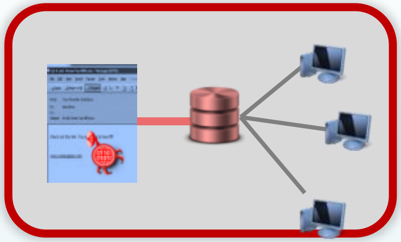
CRIMINAL ELEMENTS

TERRORIST ACTS

THREAT VECTORS

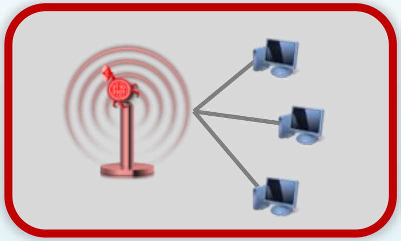
SUPPLY CHAIN VULNERABILITY

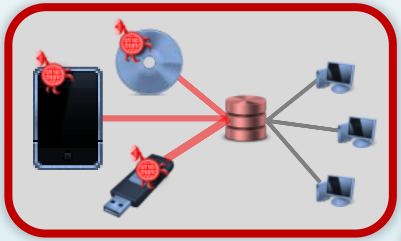




NEGLIGENT USERS

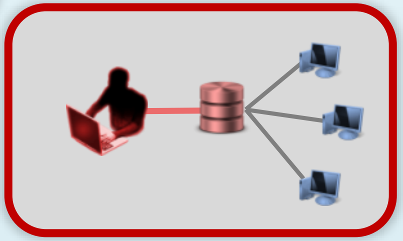
WIRELESS ACCESS POINTS





REMOVABLE MEDIA

INSIDER THREATS



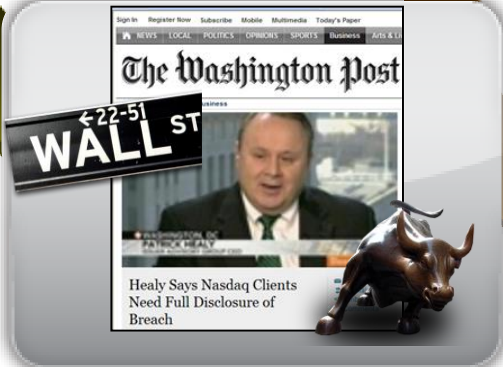
A Disturbing Trend

The Threat is Evolving

Exploitation

Disruption

Destruction

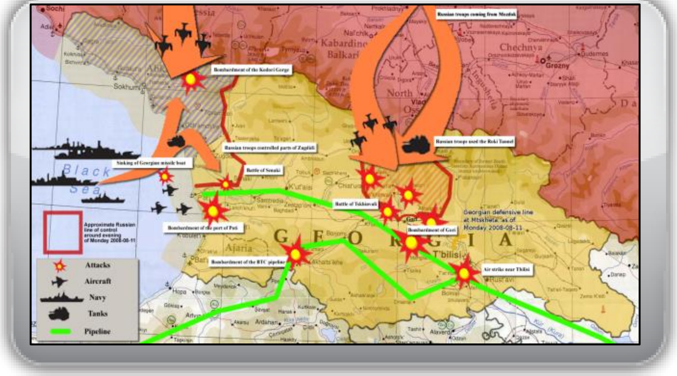


The Washington Post

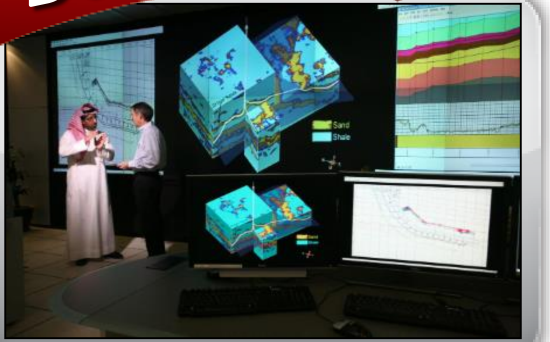
Healy Says Nasdaq Clients Need Full Disclosure of Breach

Symantec

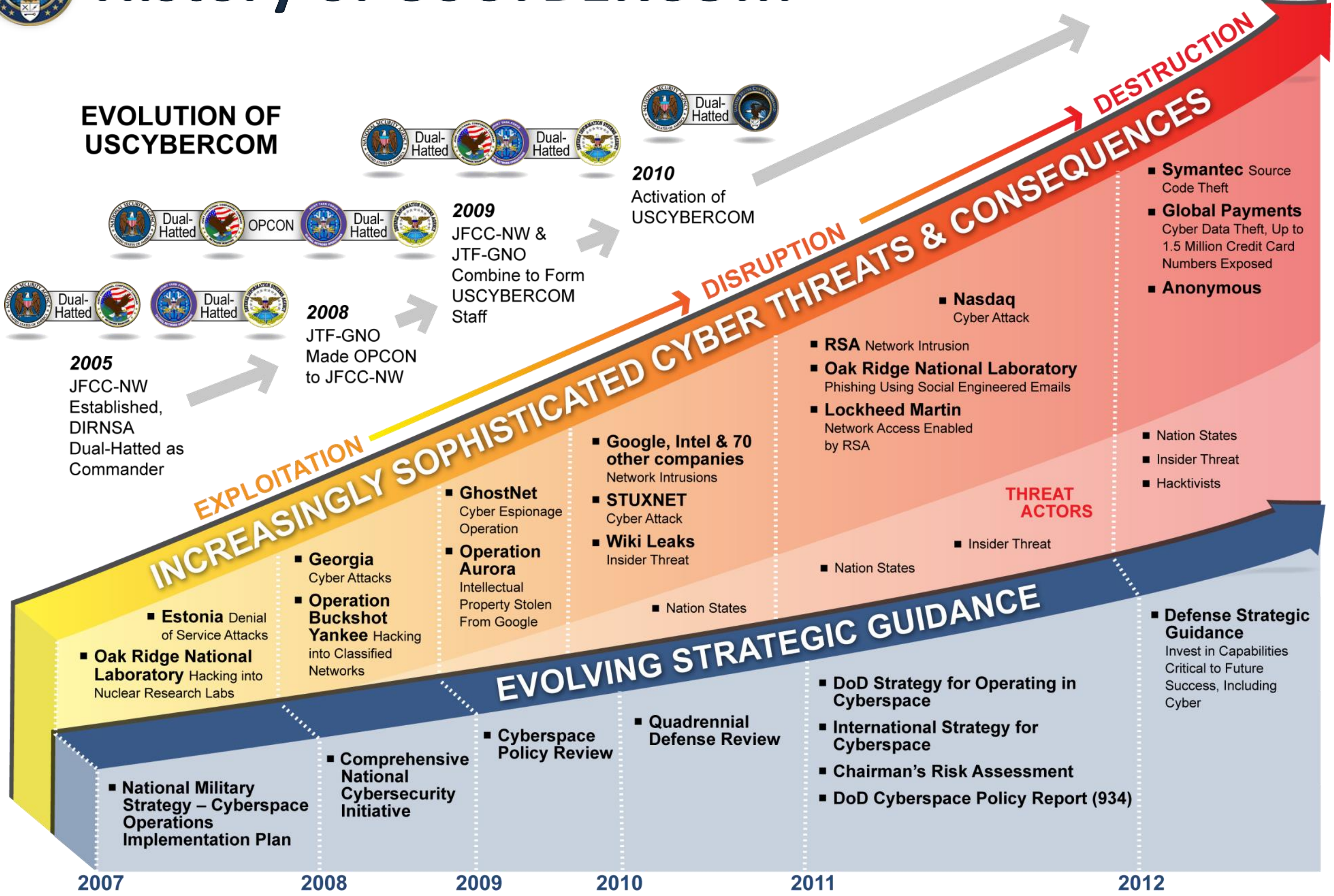
Bank of America



Sochi
Black Sea
Sokhumi
Kabardino Balkaria
Chechnya
Grozny
North Ossetia
Ingushetia
Kutaisi
Ajaria
Batumi
GEORGIA
T'bilisi
Rustavi
Gori
Bombardment of the Kodori Gorge
Russian troops coming from Mozdok
Russian troops controlled parts of Zugdidi
Russian troops used the Roki Tunnel
Sinking of Georgian missile boat
Battle of Senaki
Battle of Tskhinvali
Bombardment of the port of Poti
Bombardment of Gori
Georgian defensive line at Mtskheta as of Monday 2008-08-11
Bombardment of the BTC pipeline
Air strike near Tbilisi
Approximate Russian line of control around evening of Monday 2008-08-11
Attacks
Aircraft
Navy
Tanks
Pipeline



History of USCYBERCOM



EVOLUTION OF USCYBERCOM

2005
JFCC-NW Established, DIRNSA Dual-Hatted as Commander

2008
JTF-GNO Made OPCON to JFCC-NW

2009
JFCC-NW & JTF-GNO Combine to Form USCYBERCOM Staff

2010
Activation of USCYBERCOM

EXPLOITATION

DISRUPTION

DESTRUCTION

INCREASINGLY SOPHISTICATED CYBER THREATS & CONSEQUENCES

- **Estonia** Denial of Service Attacks
- **Oak Ridge National Laboratory** Hacking into Nuclear Research Labs

- **Georgia** Cyber Attacks
- **Operation Buckshot Yankee** Hacking into Classified Networks

- **GhostNet** Cyber Espionage Operation
- **Operation Aurora** Intellectual Property Stolen From Google

- **Google, Intel & 70 other companies** Network Intrusions
- **STUXNET** Cyber Attack
- **Wiki Leaks** Insider Threat
- Nation States

- **Nasdaq** Cyber Attack
- **RSA** Network Intrusion
- **Oak Ridge National Laboratory** Phishing Using Social Engineered Emails
- **Lockheed Martin** Network Access Enabled by RSA
- Nation States
- Insider Threat

THREAT ACTORS

- **Symantec** Source Code Theft
- **Global Payments** Cyber Data Theft, Up to 1.5 Million Credit Card Numbers Exposed
- **Anonymous**
- Nation States
- Insider Threat
- Hacktivists

EVOLVING STRATEGIC GUIDANCE

- **National Military Strategy – Cyberspace Operations Implementation Plan**
- **Comprehensive National Cybersecurity Initiative**
- **Cyberspace Policy Review**
- **Quadrennial Defense Review**
- **DoD Strategy for Operating in Cyberspace**
- **International Strategy for Cyberspace**
- **Chairman's Risk Assessment**
- **DoD Cyberspace Policy Report (934)**
- **Defense Strategic Guidance** Invest in Capabilities Critical to Future Success, Including Cyber

Business Support

US-CERT and NCCIC works among the Six Cyber Centers, federal cyber threat collaboration partners, and Information Sharing and Analysis Centers (ISACs) to analyze, build mitigation strategies for, and respond to incidents.

Information Technology ISAC

(IT-ISAC)

IT-ISAC members participate in national and homeland security efforts to strengthen the IT infrastructure through cyber information sharing and analysis.

Financial Services ISAC

(FS-ISAC)

In February 2010, the Department of Defense (DoD), DHS, and the FS-ISAC launched a pilot designed to improve the sharing of sensitive, actionable information.

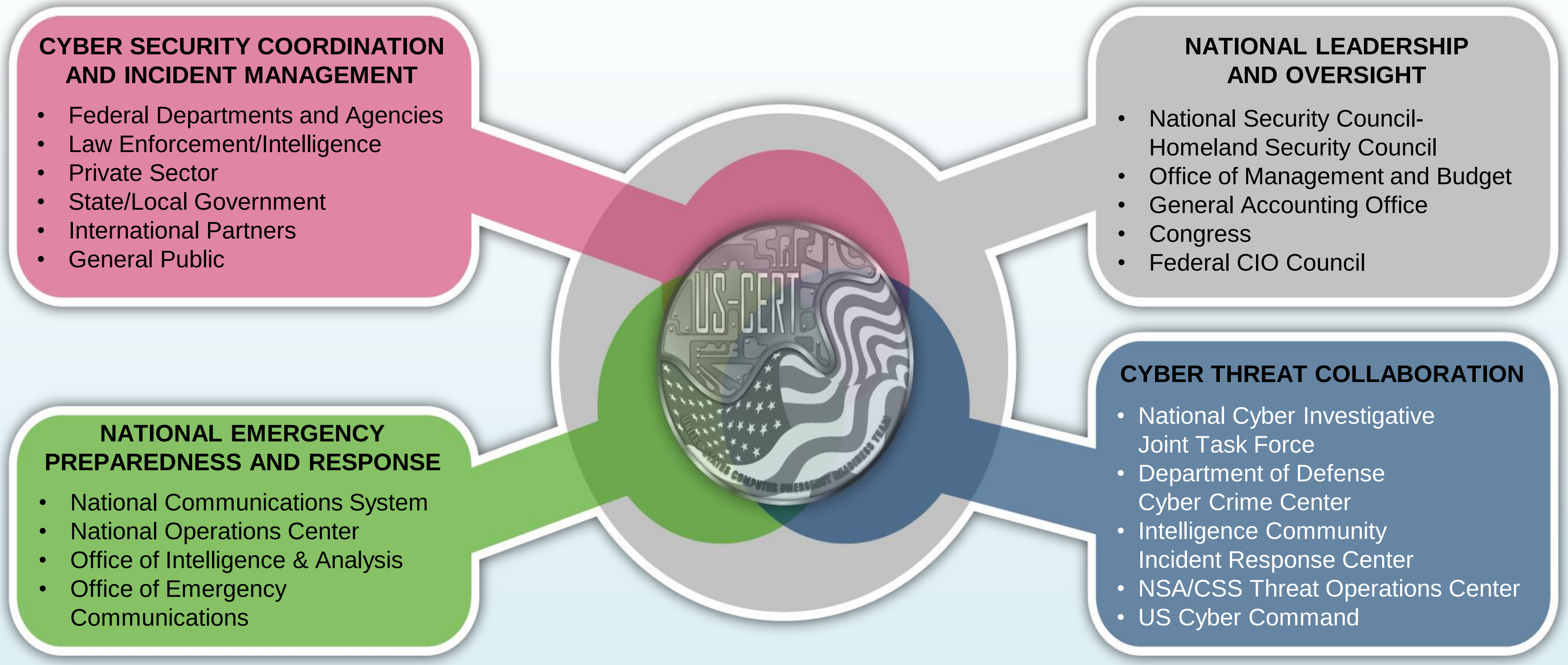
Multi-State ISAC

(MS-ISAC)

The MS-ISAC provides a common mechanism for raising the level of cybersecurity readiness and response in state, local, tribal, and territorial (SLTT) governments.

US-CERT through DHS National Cybersecurity and Communications Integration Center (NCCIC)

US-CERT gathers information on incidents affecting the Nation's cyber infrastructure and initiates two-way exchanges with each of these groups in different capacities as deemed necessary.



CYBER SECURITY COORDINATION AND INCIDENT MANAGEMENT

- Federal Departments and Agencies
- Law Enforcement/Intelligence
- Private Sector
- State/Local Government
- International Partners
- General Public

NATIONAL LEADERSHIP AND OVERSIGHT

- National Security Council-Homeland Security Council
- Office of Management and Budget
- General Accounting Office
- Congress
- Federal CIO Council

NATIONAL EMERGENCY PREPAREDNESS AND RESPONSE

- National Communications System
- National Operations Center
- Office of Intelligence & Analysis
- Office of Emergency Communications

CYBER THREAT COLLABORATION

- National Cyber Investigative Joint Task Force
- Department of Defense Cyber Crime Center
- Intelligence Community Incident Response Center
- NSA/CSS Threat Operations Center
- US Cyber Command

U.S. Department of Homeland Security

Homeland Security

THE WHITE HOUSE
WASHINGTON

National Governors Association

United States Secret Service

NATIONAL GUARD

NASCIO

MS-ISAC

Department of Justice
Federal Bureau of Investigation
Fidelity Bravery Integrity

Homeland Security Advisors

US-CERT
UNITED STATES COMPUTER EMERGENCY READINESS TEAM

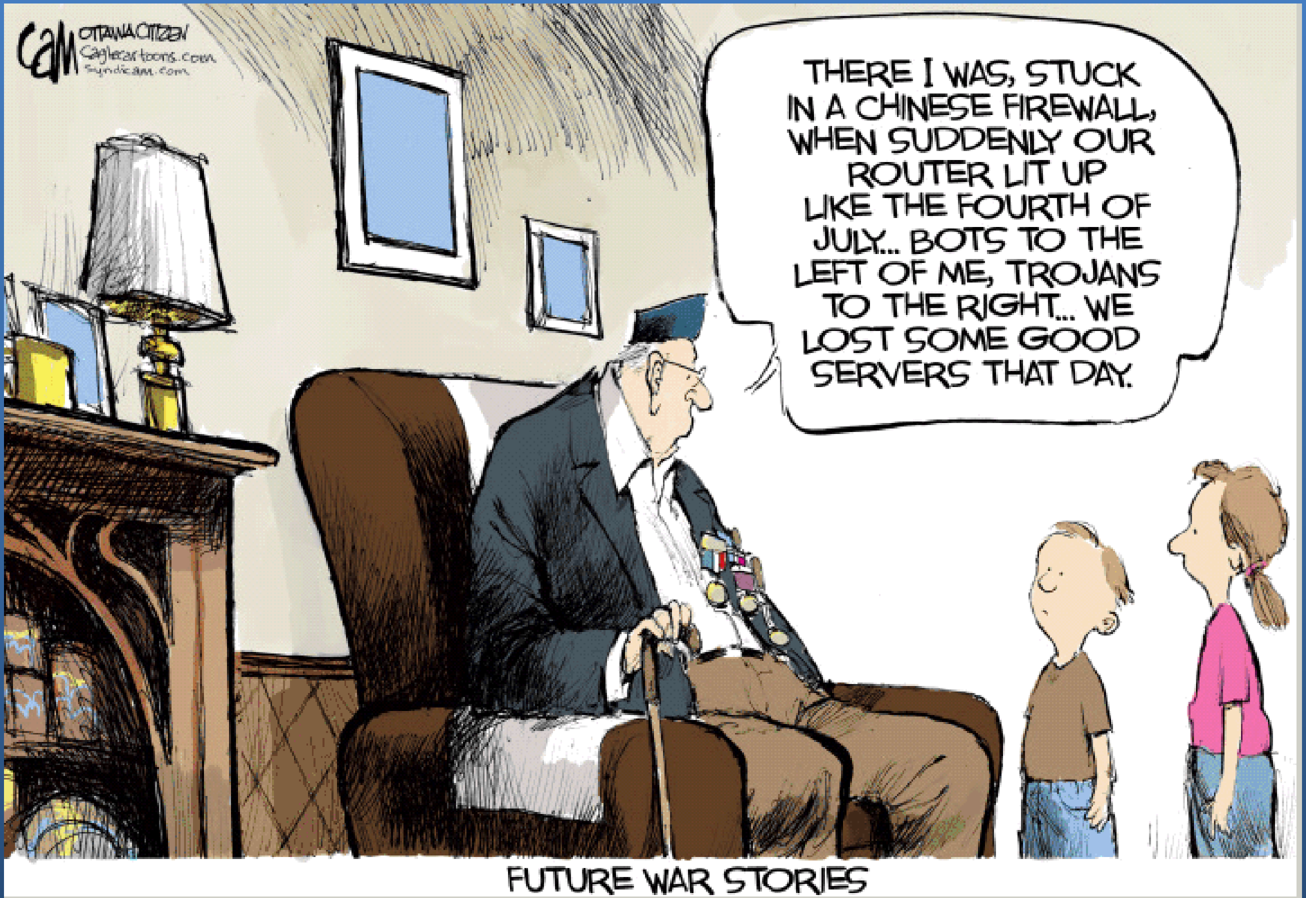
National Council of ISACs

Private Sector

National Cyber Security Division
Office of Intelligence and Analysis

E Pluribus Unum
Out of many, one

Questions?


Cam OTTAWA CITIZEN
Caglecartoons.com
syndicam.com
THERE I WAS, STUCK IN A CHINESE FIREWALL, WHEN SUDDENLY OUR ROUTER LIT UP LIKE THE FOURTH OF JULY... BOTS TO THE LEFT OF ME, TROJANS TO THE RIGHT... WE LOST SOME GOOD SERVERS THAT DAY.
FUTURE WAR STORIES

Backup

The CYBER time bomb

(U) THREAT EFFECTS

2013 Estimated Costs

- Annual cost of IP theft to US companies: $250 Billion
- Symantec estimate of costs due to global cyber crime: $388 Billion
- Amount McAfee estimates was spent globally on remediation: $1 Trillion

2013 Suspected Victims

- Defense Industry: 97
- Government Organizations: 98
- Universities & Institutes: 576
- Non-Defense Advanced Tech Sector: 1230

1/28/2013 4:37 PM